AMENDMENTS TO THE CLAIMS

1. (Previously Presented) A method for establishing a secure communication session among a first node of a network and one or more other nodes using a group shared secret key, each of the nodes having a private key value associated therewith, the method comprising the computer-implemented steps of:

communicating a first public key value of the first node to a second node;

creating and storing an initial shared secret key for the first node and second node based on a first private key value and a second public key value that is received from the second node;

creating and storing information at the first node that associates the first node with a first network communication entity by generating a collective public key value that is shared by the first node and a second node and based on the first private key value and a second private key value that is derived by the first node from the second public key value;

receiving a third public key value from a third node that seeks to join the first network communication entity;

creating a second shared secret key value based on the collective public key value and the third public key value; and

joining the first node to a second network communication entity that includes the first network communication entity and the third node and that uses secure communication with messages that are encrypted using the second shared secret key value;

wherein the first node, second node, and third node are separate nodes.

2. (Previously Presented) A method as recited in Claim 1, wherein joining the first node to a second network communication entity includes the step of communicating the first private key value to the second node and to the third node using messages encrypted using the second shared secret key value.

3. (Previously Presented) A method as recited in Claim 1, wherein creating the second shared secret key value further comprises creating and storing the second shared secret key based upon how many times each node of the second network communication entity has participated in formation of any such entity and based upon each private number of each node in the second network communication entity.

4. (Original) A method as recited in Claim 1, further comprising the step of creating and storing a subsequent shared secret key for use by the first network communication entity and the third node to enable the third node to independently compute the group shared secret key.

5. (Original) A method as recited in Claim 4, wherein creating and storing the subsequent shared secret key comprises creating and storing the subsequent shared secret key, k, according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, x = a number of times the first node has participated in entity formation, y = a number of times the second node has participated in entity formation, and z = a number of times the third node has participated in entity formation.

6. (Original) A method as recited in Claim 5, further comprising the step of storing and distributing the first public value and the second public value using a key distribution center.

7. (Original) A method as recited in Claim 5, wherein the step of joining the first node to a second network communication entity further comprises:

creating and storing a collective public key based upon the first private key value, the second private key value, and the third private key value;

communicating a collective public key of the second network communication entity to the third node.

8. (Original) A method as recited in Claim 7, wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon order of entry into the formed entity.

9. (Original) A method as recited in Claim 7, wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon a predetermined metric.

10. (Original) A method as recited in Claim 1, wherein creating and storing an initial shared secret key for the first node and second node comprises creating and storing an initial shared public key "AB" according to the relation

$$AB = k_{ab}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein k = the initial shared secret key value, a = the first private key value, b = the second private key value, p is a base value, and q is a randomly generated prime number value.

11-25. (Cancelled)

26. (Currently Amended) A computer-readable storage medium carrying one or more sequences of one or more instructions for establishing a secure communication session among a first node of a network and one or more other nodes using a group shared secret key, each of the nodes having a private key value associated therewith, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

communicating a first public key value of the first node to a second node;

creating and storing an initial shared secret key for the first node and second node based on a first private key value and a second public key value that is received from the second node;

creating and storing information at the first node that associates the first node with a first network communication entity by generating a collective public key value that is shared by the first node and a second node and based on the first private key value and a second private key value that is derived by the first node from the second public key value;

receiving a third public key value from a third node that seeks to join the first network communication entity;

creating a second shared secret key value based on the collective public key value and the third public key value; and

joining the first node to a second network communication entity that includes the first network communication entity and the third node and that uses secure communication with messages that are encrypted using the second shared secret key value;

wherein the first node, second node, and third node are separate nodes.

27. (Previously Presented) A multicast communication server for establishing a secure communication session among a first node of a network and one or more other nodes using a group shared secret key, each of the nodes having a private key value associated therewith, comprising:

means for communicating a first public key value of the first node to a second node;

means for creating and storing an initial shared secret key for the first node and second node based on a first private key value and a second public key value that is received from the second node;

means for creating and storing information at the first node that associates the first node with a first network communication entity by generating a collective public key value that is shared by the first node and a second node and based on the first private key value and a second private key value that is derived by the first node from the second public key value;

means for receiving a third public key value from a third node that seeks to join the first network communication entity;

means for creating a second shared secret key value based on the collective public key value and the third public key value;

means for joining the first node to a second network communication entity that includes the first network communication entity and the third node and that uses secure communication with messages that are encrypted using the second shared secret key value;

wherein the first node, second node, and third node are separate nodes.

28. (Previously Presented) A method as recited in Claim 1, wherein creating and storing the second shared secret key value further comprises creating and storing the second shared secret key according to the relation

$k_{abc} = (AB)^c \bmod (q) = p^{(ab)(ab)c} \bmod (q) = p^{(ab**2)c} \bmod (q)$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, AB = the collective public key value.

29. (Previously Presented) The multicast communication server in Claim 27, wherein the means for joining the first node to a second network communication entity includes means for communicating the first private key value to the second node and to the third node using messages encrypted using the second shared secret key value.

30. (Previously Presented) The multicast communication server in Claim 27, wherein the means for creating the second shared secret key value further comprises means for creating and storing the second shared secret key based upon how many times each node of the second network communication entity has participated in formation of any such entity and based upon each private number of each node in the second network communication entity.

31. (Previously Presented) The multicast communication server in Claim 27, further comprising means for creating and storing a subsequent shared secret key for use by the

first network communication entity and the third node to enable the third node to independently compute the group shared secret key.

32. (Previously Presented) The multicast communication server in Claim 31, wherein the means for creating and storing the subsequent shared secret key comprises means for creating and storing the subsequent shared secret key, k, according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, x = a number of times the first node has participated in entity formation, y = a number of times the second node has participated in entity formation, and z = a number of times the third node has participated in entity formation.

33. (Previously Presented) The multicast communication server in Claim 32, further comprising means for storing and distributing the first public value and the second public value using a key distribution center.

34. (Previously Presented) The multicast communication server in Claim 32, wherein the means for joining the first node to a second network communication entity further comprises:

means for creating and storing a collective public key based upon the first private key value, the second private key value, and the third private key value;

means for communicating a collective public key of the second network communication entity to the third node.

35. (Previously Presented) The multicast communication server in Claim 34, wherein the means for joining the first node to a second network communication entity further comprises means for determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon order of entry into the formed entity.

36. (Previously Presented) The multicast communication server in Claim 34, wherein the means for joining the first node to a second network communication entity further comprises means for determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon a predetermined metric.

37. (Previously Presented) The multicast communication server in Claim 27, wherein the means for creating and storing an initial shared secret key for the first node and second node comprises means for creating and storing an initial shared public key "AB" according to the relation

$$AB = k_{ab}{}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein k = the initial shared secret key value, a = the first private key value, b = the second private key value, p is a base value, and q is a randomly generated prime number value.

38. (Previously Presented) The multicast communication server in Claim 27, wherein the means for creating and storing the second shared secret key value further comprises means for creating and storing the second shared secret key according to the relation

$k_{abc} = (AB)^c \bmod (q) = p^{(ab)(ab)c} \bmod (q) = p^{(ab**2)c} \bmod (q)$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, AB = the collective public key value.

39. (Previously Presented) An apparatus for establishing a secure communication session among a first node of a network and one or more other nodes using a group shared secret key, each of the nodes having a private key value associated therewith, comprising:

one or more processors;

a computer-readable storage medium carrying one or more sequences of one or more instructions, the one or more sequences of one or more instructions including

instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

communicating a first public key value of the first node to a second node;

creating and storing an initial shared secret key for the first node and second node based on a first private key value and a second public key value that is received from the second node;

creating and storing information at the first node that associates the first node with a first network communication entity by generating a collective public key value that is shared by the first node and a second node and based on the first private key value and a second private key value that is derived by the first node from the second public key value;

receiving a third public key value from a third node that seeks to join the first network communication entity;

creating a second shared secret key value based on the collective public key value and the third public key value;

joining the first node to a second network communication entity that includes the first network communication entity and the third node and that uses secure communication with messages that are encrypted using the second shared secret key value;

wherein the first node, second node, and third node are separate nodes.

40. (Previously Presented) An apparatus as recited in Claim 39, wherein the step of joining the first node to a second network communication entity includes the step of communicating the first private key value to the second node and to the third node using messages encrypted using the second shared secret key value.

41. (Previously Presented) An apparatus as recited in Claim 39, wherein the step of creating the second shared secret key value further comprises creating and storing the second shared secret key based upon how many times each node of the second network

communication entity has participated in formation of any such entity and based upon each private number of each node in the second network communication entity.

42. (Previously Presented) An apparatus as recited in Claim 39, the one or more sequences of one or more instructions including instructions which, when executed by the one or more processors, cause the one or more processors to further perform the step of creating and storing a subsequent shared secret key for use by the first network communication entity and the third node to enable the third node to independently compute the group shared secret key.

43. (Previously Presented) An apparatus as recited in Claim 42, wherein creating and storing the subsequent shared secret key comprises creating and storing the subsequent shared secret key, k, according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, x = a number of times the first node has participated in entity formation, y = a number of times the second node has participated in entity formation, and z = a number of times the third node has participated in entity formation.

44. (Previously Presented) An apparatus as recited in Claim 43, the one or more sequences of one or more instructions including instructions which, when executed by the one or more processors, cause the one or more processors to further perform the step of storing and distributing the first public value and the second public value using a key distribution center.

45. (Previously Presented) An apparatus as recited in Claim 43, wherein the step of joining the first node to a second network communication entity further comprises:
creating and storing a collective public key based upon the first private key value, the second private key value, and the third private key value;

communicating a collective public key of the second network communication entity to the third node.

46. (Previously Presented) An apparatus as recited in Claim 45, wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon order of entry into the formed entity.

47. (Previously Presented) An apparatus as recited in Claim 45, wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon a predetermined metric.

48. (Previously Presented) An apparatus as recited in Claim 39, wherein creating and storing an initial shared secret key for the first node and second node comprises creating and storing an initial shared public key "AB" according to the relation

$$AB = k_{ab}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein k = the initial shared secret key value, a = the first private key value, b = the second private key value, p is a base value, and q is a randomly generated prime number value.

49. (Previously Presented) An apparatus as recited in Claim 39, wherein creating and storing the second shared secret key value further comprises creating and storing the second shared secret key according to the relation

$$k_{abc} = (AB)^{c} \bmod (q) = p^{(ab)(ab)c} \bmod (q) = p^{(ab**2)c} \bmod (q)$$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, AB = the collective public key value.